



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/893,461	06/29/2001	Michael Thomas Kurdziel	HAR65 001	6363
7590	09/20/2005		EXAMINER	
DUANE MORRIS LLP			BROWN, CHRISTOPHER J	
1667 K STREET NW				
SUITE 700			ART UNIT	PAPER NUMBER
WASHINGTON, DC 20006			2134	

DATE MAILED: 09/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

TH

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/893,461	KURDZIEL, MICHAEL THOMAS	
	Examiner Christopher J. Brown	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 6/24/2005.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 4-10 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 4-10 is/are rejected.  
 7) Claim(s) 4,5,6,8,10 is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____

## **DETAILED ACTION**

### ***Response to Arguments***

1. Applicant's arguments filed 6/24/2005 have been fully considered but they are not persuasive.

As per the examiners argument that the term “responsive” must be read in light of the other words in the claim is not persuasive. The term responsive is vague and indefinite.

The applicant is requested to be more *specific* with regards to the invention. For example, in Claim 7 a “key scheduler is responsive to a key data block” there is no action in this statement. What does responsive mean? Does the key scheduler start because of the key data block? Does it use data from the key data block? Does the key scheduler stop because of the key data block?

Further in claim 7 the statement “a first function unit responsive to a first portion of the key data block for producing a first key data sub-block;” It is unclear how the first function unit is “responding” to the first portion of the key data block. Again, Is there a cause and effect relationship? Is the first function unit using data from the first portion of the key data block?

The term “responsive” is unreasonably broad. The use of the term “responsive” in Claims 4, 6, 7, and 8 should be removed and replaced with more descriptive language.

The examiner would like to make of record that by stating “the improvement” in claim 8, the applicant is admitting that anything previous to “the improvement” is prior art.

In addition to the applicant’s unpersuasive argument with regards to the 35 U.S.C. 112 rejection regarding the term “responsive” the applicant *has not addressed any of the Examiners Objections and has not addressed multiple 35 U.S.C. 112 Rejections.*

The 35 USC § 103 rejection is maintained in view of the numerous outstanding objections not addressed.

These Objections and Rejections will be repeated below.

### ***Claim Objections***

1. Claims 4, 6, 8, are objected to because of the following informalities: The claim lacks a transitional phrase. These claims do not contain a preamble to the claims. Independent Claim 7 is the only independent claim containing a preamble. Appropriate correction is required.

Claims 4, 6, and 8’s first line statements contain phrases that are not correct English. For example Claim 4 states “In a plural block cipher device cryptographically secured digital communication system having....” at the very least there should be “a” between “device”

and “cryptographically” Preferably the statement should read more along the lines “A cryptographically secured digital communication system containing a plural block cipher device wherein at least one block cipher....” Claims 6, and 8 also must be corrected.

Claim 4 is objected to because of the following informalities: line 8 consists of the sentence “...the operation of the most downstream of the modulo operators ...” The examiner assumes that the sentence should read “...the operation of most downstream modulo operators...” The sentence is not comprehensible as is. Appropriate correction is required.

Claim 4 recites “one block cipher device” in lines 2 and 4, it is unclear whether the applicant intended these devices to be the same block cipher device or different. The examiner recommends labeling a first and second device. Appropriate correction is required.

Claim 4 recites “a block cipher device” in lines 6 and 7, it is unclear whether the applicant intended these devices to be the same block cipher device or different. The examiner recommends labeling a first and second device. Appropriate correction is required.

Claim 4 is objected to because the claim starts out as a “system” claim, and on line 6 continues as a “method” claim. It is unclear if the claim is a system or method. Appropriate correction is required.

Claim 5 recites the limitation "the first block cipher" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 5 recites the limitation "the second block cipher" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 6 recites a "system" in line 2 and a "method" in line 2 it is unclear if this is a system or method claim. Appropriate correction is required.

Claim 6 recites "a block cipher device", "at least one block cipher device" and "a block cipher device" on lines 2, 3, and 4. It is unclear whether these devices are the same or different. A clearer distinction between devices is required.

Claim 6 recites a "second selectively variable fixed length...." That is one half the length of the first key. The examiner believes there is a noun missing after "length" because the statement is not understandable otherwise. Appropriate correction is required.

Claim 6 recites "first key generator in two equal sections" it is not clear if "in" means there is a key generator duplicated in 2 sections, or that a first key generator has two equal sections. Appropriate correction is required.

Claim 6 recites "the second key generator" in step (a) There is insufficient antecedent basis for this limitation in the claim. Appropriate correction is required.

Claim 6 recites “the second key” in step (b) There is insufficient antecedent basis for this limitation in the claim. Appropriate correction is required.

Claim 10 is objected to because of the following informalities: The claim depends on a non-existent “Claim 11” Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 4, 6, 7, and 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The use of the word “responsive” is vague and indefinite. The examiner recommends a more descriptive word, or phrase regarding the invention.

Claim 8 recites the limitation “the improvement” in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claims 5, 9 and 10 are rejected based on their dependence on rejected independent claims.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore US 6,061,449 in view of Coutts US 5,835,603.

As per claims 1, 4, and 6 Candelore teaches using a public/private key algorithm in a block cipher encryption/ decryption system, (Col 32 lines 1-15). Candelore does not specifically teach using a fixed length set of keys.

Coutts teaches using fixed length keys with various well known cryptographic algorithms, (Col 3 lines 34-38).

It would have been obvious to one skilled in the art to use the teachings of Coutts with Candelore because the algorithms taught in Coutts are well known and secure.

Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore US 6,061,449 in view of Coutts US 5,835,603 in view of Matyas US 5,201,000 As per claims 2, 3, and 5 The previous Candelore-Coutts combination does not teach specified key length.

Art Unit: 2134

Matyas teaches using an algorithm to generate a key pair of whatever bit length is desired, (col 14 lines 8-13).

It would have been obvious to generate different but key lengths based on the public private key algorithm in Candelore-Coutts.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore US 6,061,449 in view of Coutts US 5,835,603 in view of Lim US 2002/0018562

The previous Candelore-Coutts combination does not teach a key scheduler.

Lim teaches a key scheduler generating two subkeys, [0031].

It would have been obvious to one skilled in the art to use the teachings of Lim with the system of Candelore-Coutts because the key scheduler generates a plurality of keys.

### *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

Art Unit: 2134

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

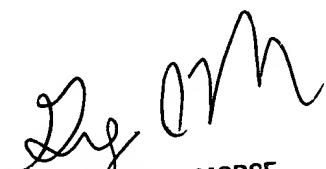
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher J. Brown

9/13/05



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100